

WHAT IS CLAIMED IS:

- 1 1. A system for performing cryptographic operations on network data, the
2 system comprising:
3 an input interface configured to receive data into the system;
4 a plurality of processors in a cascaded arrangement, each processor having
5 an input coupled to the input interface and an output coupled to respective inputs of each
6 of the other processors downstream in the arrangement, the processors each configured to
7 perform respective cryptographic operations on the data; and
8 an output interface coupled to the input interface and to the output of each
9 of the processors, the output interface configured to transmit data out of the system and to
10 direct the data through the system in coordination with the input interface according to a
11 predetermined algorithm.
- 1 2. The system of claim 1, wherein the plurality of processors comprises:
2 a first processor having its data inputs coupled only to the input interface,
3 the first processor configured to compress uncompressed data and to decompress
4 compressed data.
- 1 3. The system of claim 2, wherein the first processor is configured to
2 compress and decompress the data according to at least one of a Lempel-Ziv-Stac (LZS)
3 and an Adaptive Lossless Data Compression (ALDC) compression algorithm.
- 1 4. The system of claim 2, wherein the plurality of processors comprises:
2 a second processor having a first input coupled to the input interface and a
3 second input coupled to an output of the first processor, the second processor configured
4 to obscure non-secure data and to decipher secure data.
- 1 5. The system of claim 4, wherein the second processor is configured to
2 obscure and decipher the data according to at least one of a Data Encryption Standard
3 (DES), a Triple-DES, and an Advanced Encryption Standard (AES) algorithm.
- 1 6. The system of claim 4, wherein the plurality of processors comprises:

2 a third processor having a first input coupled to the input interface, a
3 second input coupled to an output of the first processor, and a third input coupled to an
4 output of the second processor, the third processor configured to determine an integrity of
5 the data.

1 7. The system of claim 6, wherein the third processor is configured to
2 determine the integrity by hashing the data according to at least one of a Secure Hash
3 Algorithm (SHA-1) and a Message Data 5 (MD5) algorithm.

1 8. The system of claim 1, wherein the predetermined algorithm is based on
2 control information included in a security association related to the data.

1 9. The system of claim 8, wherein the input interface is configured to receive
2 the control information and to forward the control information to each of the processors
3 for use in performing the respective cryptographic operations on the data.

1 10. The system of claim 9, wherein the control information includes at least
2 one of:

3 an identity of an authentication algorithm used to hash the data;
4 an identity of an encryption algorithm used to obscure and decipher the
5 data;

6 keying material used by at least one of the authentication and encryption
7 algorithms; and

8 a lifetime of the security association related to the data.

1 11. The system of claim 1, comprising:
2 logic configured to determine a checksum associated with the data
3 transmitted out of the system.

1 12. A method for performing cryptographic operations on network data, the
2 method comprising:
3 receiving data;

4 directing the received data through a cascaded arrangement of processors
5 according to a predetermined algorithm, each processor having an input coupled to the
6 received data and an output coupled to respective inputs of each of the other processors
7 downstream in the arrangement;
8 performing respective cryptographic operations defined by the
9 predetermined algorithm on the received data using the plurality of processors; and
10 transmitting the operated-on data after performing the cryptographic
11 operations defined by the predetermined algorithm.

1 13. The method of claim 12, comprising:
2 compressing uncompressed received data and decompressing compressed
3 received data using a first processor in the arrangement having its data inputs coupled
4 only to the received data.

1 14. The method of claim 13, comprising:
2 compressing and decompressing the received data according to at least one
3 of a Lempel-Ziv-Stac (LZS) and an Adaptive Lossless Data Compression (ALDC)
4 compression algorithm.

1 15. The method of claim 13, comprising:
2 obscuring non-secure data and deciphering secure data using a second
3 processor in the arrangement having a first input coupled to the received data and a
4 second input coupled to an output of the first processor.

1 16. The method of claim 15, comprising:
2 obscuring and deciphering the data according to at least one of a Data
3 Encryption Standard (DES), a Triple-DES, and an Advanced Encryption Standard (AES)
4 algorithm.

1 17. The method of claim 15, comprising:
2 determining an integrity of the data using a third processor in the
3 arrangement having a first input coupled to the received data, a second input coupled to

4 an output of the first processor, and a third input coupled to an output of the second
5 processor.

1 18. The method of claim 17, comprising:
2 hashing the data to determine the integrity according to at least one of a
3 Secure Hash Algorithm (SHA-1) and a Message Data 5 (MD5) algorithm.

1 19. The method of claim 12, comprising:
2 determining the predetermined algorithm based on control information
3 included in a security association related to the received data.

1 20. The method of claim 19, comprising:
2 receiving the control information; and
3 forwarding the control information to each of the processors for use in
4 performing the respective cryptographic operations on the data.

1 21. The method of claim 20, comprising:
2 including in the control information at least one of:
3 an identity of an authentication algorithm used to hash the data;
4 an identity of an encryption algorithm used to obscure and
5 decipher the data;
6 keying material used by at least one of the authentication and
7 encryption algorithms; and
8 a lifetime of the security association related to the data.

1 22. The method of claim 12, comprising:
2 determining a checksum associated with the transmitted data.

1 23. A computer readable medium containing a computer program for
2 performing cryptographic operations on network data, wherein the computer program
3 comprises executable instructions for:
4 receiving data;

5 directing the received data through a cascaded arrangement of processors
6 according to a predetermined algorithm, each processor having an input coupled to the
7 received data and an output coupled to respective inputs of each of the other processors
8 downstream in the arrangement;
9 performing respective cryptographic operations defined by the
10 predetermined algorithm on the received data using the plurality of processors; and
11 transmitting the operated-on data after performing the cryptographic
12 operations defined by the predetermined algorithm.

1 24. The computer readable medium of claim 23, wherein the computer
2 program comprises executable instructions for:
3 compressing uncompressed received data and decompressing compressed
4 received data using a first processor in the arrangement having its data inputs coupled
5 only to the received data;
6 obscuring non-secure data and deciphering secure data using a second
7 processor in the arrangement having a first input coupled to the received data and a
8 second input coupled to an output of the first processor; and
9 determining an integrity of the data using a third processor in the
10 arrangement having a first input coupled to the received data, a second input coupled to
11 an output of the first processor, and a third input coupled to an output of the second
12 processor.

1 25. The computer readable medium of claim 24, wherein the computer
2 program comprises executable instructions for:
3 compressing and decompressing the received data according to at least one
4 of a Lempel-Ziv-Stac (LZS) and an Adaptive Lossless Data Compression (ALDC)
5 compression algorithm;
6 obscuring and deciphering the data according to at least one of a Data
7 Encryption Standard (DES), a Triple-DES, and an Advanced Encryption Standard (AES)
8 algorithm; and

9 hashing the data to determine the integrity according to at least one of a
10 Secure Hash Algorithm (SHA-1) and a Message Data 5 (MD5) algorithm.

1 26. The computer readable medium of claim 23, wherein the computer
2 program comprises executable instructions for:
3 determining the predetermined algorithm based on control information
4 included in a security association related to the received data;
5 receiving the control information; and
6 forwarding the control information to each of the processors for use in
7 performing the respective cryptographic operations on the data.

1 27. The computer readable medium of claim 23, wherein the computer
2 program comprises executable instructions for:
3 determining a checksum associated with the transmitted data.